PBOT: Automotus

Privacy Impact Assessment

Status: Released version

Smart City PDX

November 14, 2024

PRIVACY IMPACT ASSESSMENT REPORT

City of Portland Privacy Toolkit

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A Privacy Impact Assessment ("PIA") is a method to quickly evaluate the general privacy risks of a technological solution or a specific use, transfer, or collection of data to City bureaus or offices. The PIA is a way to identify factors that contribute to privacy impacts and risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Assessment may lead to a more comprehensive Surveillance Assessment depending on the level or risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency about data collection and management, the City of Portland has committed to publishing all Privacy Impact Assessments on an outward facing website for public access. PIAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS A THRESHOLD PRIVACY IMPACT ASSESSMENT RECOMMENDED?

A PIA is recommended when:

- A project, technology, data sharing agreement, or other review has been flagged as having some privacy risk due to the collection of private or sensitive data.
- A technology has high financial impact and includes the collection, use or transfer of data by city bureaus or third parties working for or on behalf of the city.

HOW TO COMPLETE THIS DOCUMENT.

A PIA consists of two sections:

- *The Privacy Analysis.* This portion identifies all important information related to the project description, data collection, use, safekeeping, and management; as well as a verification of existing privacy policies and measures to protect private information. This report is a summary of the analysis.
- *The Comprehensive Privacy Risk Assessment.* This portion breaks the privacy risk into six different Risk Types of evaluation: (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact. It then compares those risks to their likelihood of occurring to create a single risk measure based on the worst-case scenario.

Executive summary

This document presents the privacy impact assessment of *Automotus*' camera system for the Zero-Emission Delivery Zone pilot project headed by the Portland Bureau of Transportation (PBOT). This project has a medium to low risks.

The purpose of the pilot project is to incentivize businesses to adopt zero-emission vehicles for last-mile deliveries. The pilot stretches within a designated 15 blocks in downtown Portland. To understand who uses exclusive delivery zones, measure traffic reduction, and other metrics, PBOT is assessing *Automotus*' solution for safely collecting these metrics.

Automotus uses cameras attached to street poles to identify zero-emission vehicles registered with the pilot project, and the length of their stay, by identifying their license plate, vehicle make and model, or visible QR Code. After collecting and identifying these identifiers, with no intervention from employees, their system anonymizes the data by deleting any personally identifiable information (PII) from the database using machine learning. This deidentification process has been audited by a third-party.[1] This application does not collect face biometric information.

The remaining metadata consists of statistics about the vehicles, zero-emission vehicles, persons, vehicle arrivals/departures and double parking. All this processing occurs at the edge (at or near the point of collection), reducing the risks arising from sending information to distal databases and risks related to retaining PII.

Notable risks identified include vandalism and low transparency. Because these cameras will be installed in the public right of way by streetlights, there is a chance someone can disrupt them.

The risk of vandalism is low, given that the location of these cameras is high up at the lighting post level. However, the risk of vandalism is always present, and the bureau and vendor are ready to services any potential device that requires it.

Additionally, those walking by may see the camera and wonder what the purpose of it is. PBOT is already working on public signage that describes the camera and the project. Cameras could cause a chilling effect (a change in behavior due to being observed).

This application was identified to have a Medium risk worst-case scenario. This is due to the use of public interest technology and the possibility of using this information for other purposes. However, the collection of information from license plate readers is

[1] https://www.automotus.co/

limited to processing in the device and this pilot also constrains information use only to this application. The application of this service is proportional to the need and makes parking identification more effective. (see Proportionality and Necessity notes below).

The following table summarizes the outcome of privacy risks to the city.

Risk area	Risk level determined	Highlighted risks
Individual Privacy Harms	Medium	Risk of using data for other purposes.
Equity, Disparate Community Impact	-	No major risk was identified due to the scale of the pilot.
Political, Reputation & Image	Medium	Image and reputation damage due to misuse of the technology
City Business, Quality & Infrastructure	Low	Vandalism, theft, or destruction.
Legal & Regulatory	Low	Legal risks due to privacy or sensitive information breach
Financial Impact	Low	Risks of too expensive commissioning, maintenance, and Decommissioning Costs

Privacy Analysis

Purpose of the technology, project, data sharing or application

PROJECT
The Infrastructure Investment and Jobs Act (2021) established the Strengthening Mobility and Revolutionizing Transportation (SMART) Grant Program under Title V of the Act – Research and Innovation.

"The SMART Grants Program was established to conduct demonstration projects focused on advanced smart city or community technologies and systems that will improve transportation efficiency and safety. The program seeks to fund purpose-driven innovation and focuses on building data and technology capacity and experience for State, local, and Tribal governments" (US DOT).

"The SMART Grants Program is divided into two stages. These stages are Stage 1: Planning and Prototyping Grants and Stage 2: Implementation Grants. During Stage 1, recipients should build internal buy-in and partnerships with stakeholders to refine and prototype their concepts, and report on results. Stakeholders can include public, private, academic, and nonprofit organizations; organized labor and workforce organizations; and community organizations and networks. At the conclusion of Stage 1, awardees should have the information to either create a fully realized implementation plan with robust performance metrics; or to make an informed decision not to proceed with the concept. Stage 1 results may uncover previously unknown institutional barriers, technical limitations, or poor performance relative to conventional solutions. USDOT anticipates that Stage 1 will award grantees up to approximately $2 million over up to 18 months" (US DOT).[2]

ZERO-EMISSION DELIVERY ZONES
The City of Portland and the Portland Bureau of Transportation (PBOT) recognize the importance of freight decarbonization initiatives, such as the Zero-Emission Delivery Zone (ZEDZ) pilot project, to make progress towards the City and Bureau's climate, public health, and safety outcomes. Transportation accounts for nearly 40% of the carbon emissions in the Portland area and, although trucks represent less than 5% of the vehicle fleet, they generate 24% of all transportation-related GHG emissions. Portland's downtown core was identified among the areas with the highest concentration of truck-involved collisions. Nearly 40% of Black, Indigenous and People of Color in Portland live within 1.2 miles of the city's biggest sources of air pollution, like

[2] https://www.transportation.gov/grants/SMART

freeways and industrial facilities. An effective ZEDZ and other clean last-mile solutions will enhance livability, safety, boost economic opportunities for zero emissions carriers while also mitigating negative externalities (e.g., air pollution, traffic collisions, and carbon emissions).

Sustainable freight goals for the City of Portland are outlined in the City Council-adopted Climate Emergency Workplan, Transportation Decarbonization Strategies Resolution, and the 2040 Freight Plan. [3]

Technology
Cameras are used to detect unique identifiers on the vehicle (e.g., QR Code, Make/Model) using the piloted Zero-Emission Commercial Delivery Zones and how the identified piloted curbs are being used. Deidentified data about curb activity and street traffic (i.e., metadata) are used to deliver aggregated and de-identified statistics to city transportation agencies for policy creation that would lead to reduced congestion, emissions, and safety hazards in high-traffic areas.

Name of the entity owner of the application and website

Automotus

Type of Organization
Private Company

Scope of personal data collected. List all sources of data and information

PERSONAL DATA
Vehicle License Plate (text, state). License plate information is only collected to identify a vehicle and it is then deleted.

SOURCES
Camera's Field of View.

How is personal data collected?

3
https://www.congress.gov/bill/117th-congress/house-bill/3684
https://www.transportation.gov/grants/SMART
https://www.portland.gov/transportation/planning/zero-emission-delivery/zero-emission-delivery-zone

A camera is set up on public infrastructure (e.g., street signal) and is directed toward the curb or relevant loading zones.

Who can access the data?

Only authorized and trained vendor staff can view metadata (data about data) not containing personally identifiable information (PII). The staff at PBOT or INRIX (a data processor under contract with the City) can only access aggregated statistics.

Purposes the data is used for and data lifecycle

PURPOSE
Data is used for developing insights for PBOT. Information collected by this project will **NOT** be shared with police or used for parking enforcement.

DATA LIFECYCLE
First, images are captured and then de-identified immediately using Machine Learning (ML). De-identified images are tagged with metadata that identifies cars, persons, e-bikes, trikes and other street and pedestrian traffic as well as events such as parking, double parking and exits. Identified objects are then collected and aggregated for statistics available via an API for the Portland Bureau of Transportation. License plate information will not be retained or used for parking enforcement during any stage of the project. The remaining anonymized data may be retained according to data retention practices of *Automotus* and the City.

DATA COLLECTION PROCESS
Identification of authorized vehicles in zero-emissions parking spot starts by collecting images with a camera. A collection of cameras may be able to track a vehicle based on unique features. Identifying a vehicle involves a combination of license plate readers, features identification, and specific tags or numbers attached to the vehicle.

Zero-emission parking spots can only be occupied by authorized commercial vehicles. So, a process that delivers a unique id number that matches features of a list of authorized vehicles will validate the specific parking. Otherwise, it will flag unauthorized use of the parking spot.

Where is the data stored?

Data is stored on *Automotus*' cloud and processed on City's servers. The City will generate derivative datasets from the analysis from data in this period. At the end of life

of this project, data stored in the vendor cloud may be destroyed after a specific timeline.

How is data shared?
Data is shared via an Open API, specifically “Curb Data Specification.”

“CDS— ‘Curb Data Specification’ —is a digital tool that helps cities and companies pilot and scale dynamic curb zones. CDS provides a mechanism for expressing static and dynamic regulations, measuring activity at the curb, and developing policies that create more accessible, useful curbs.”[4]

What data does the City share?

The City will share results with stakeholders. It also plans on communicating via surveys and interviews with community members (e.g., property owners, tenants) and organizational stakeholders (e.g., freight and goods movement stakeholders) to address on-the-ground problems that may emerge. Data will also be available via a publicly available dashboard.

How long is the data stored?

Images/video containing Personally Identifiable Information are deleted after identifying objects and creating statistics from them. Aggregated statistics are held until the end of the retention schedule. Aggregated anonymous statistics can be held indefinitely without significant risk of re-identification (e.g., 57% of Portland State students are female).

Effectiveness

Environmental conditions may reduce the effectiveness of the camera. The effectiveness of these sensors depends on the installation factors like obstructions, field of view and distance to the area of interest. The accuracy of their machine learning model will affect the effectiveness of their deidentification process.

Santa Monica and Pittsburgh have adopted the technology. The following case studies were reported by the vendor. In Santa Monica, the cameras identified a street with the highest number of double parking and the longest duration of double parking as well as the time of their peaks. Using this information, Santa Monica could add more parking in

---

4 https://www.openmobilityfoundation.org/about-cds/
https://github.com/openmobilityfoundation/curb-data-specification

the surrounding area to reduce double parking. Similar findings and recommendations were found by Pittsburgh. [5]

Proportionality and Necessity

Our use of the term “Proportionality and Necessity” refers to whether the means of collection and the data collected are necessary to complete a specified aim, that is, not collecting, retaining, or sharing more information than necessary to obtain statistics for curb and zero-emission policy; and to consider if there are less intrusive but equally effective ways to complete a specified aim. A technology could be said to be proportional if the data used does not pose an outsized risk compared to the benefits gained from the technology.

Benefits: Provides cities with insights, automated payment and enforcement solutions to manage rise in commercial vehicle congestion and emissions. Creates smarter curbside policies. Creates designated unloading zones, reducing congestion and safety hazards. Cameras may reduce costs for PBOT on curb management. Cons: See Risks.

With a minimal amount of data collected and current de-identification practices there is a great proportionality ratio for the aim of collecting statistics for curb and zero-emission policy. An alternative to deploying cameras is hiring parking enforcement personnel but this method may include higher costs and a risk of potential miscounts. As there is a minimal amount of data retained, and what is retained is anonymized, there is little more the vendor can do to mitigate privacy risks.

Privacy safeguards

De-identification, Data Minimization, Use Limitation, Access Controls and Training.

1. Deidentification of non-relevant information
2. Data Minimization (Video streams are processed in real time and then deleted instantly). No PII is collected. All curb information is de-identified, even faces. Non-relevant license plates, faces and all images are deleted immediately once payment or citation is resolved (no ticketing will take place under the pilot).
3. Access Controls: Access through API is restricted by access token, so only individuals who have tokens are granted access.
4. Training: individuals at *Automotus* with access to metadata undergo training.

---

5 https://www.automotus.co/pittsburgh-smart-loading-zones-case-study
https://www.automotus.co/santa-monica-case-study

Open source

The vendor's platform is proprietary. Curb Data Specification API is open.

AI/ML claims

Yes. ML is used to generate metadata and guide de-identification efforts.

Privacy Policy Link

https://www.automotus.co/privacypolicy

Surveillance Tech

Yes

Portland Privacy Principles (P3)

Data Utility: *All Information and Data processes must bring value to the City of Portland and the communities the City serves. The City will collect only the minimum amount of Personal Information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.*

All personal Information collected is de-identified and its sole purpose is generating statistics for future decisions that will benefit the stakeholders and communities involved. The minimal amount of data collected is for the completion of this project and any PII is deleted. No audio or biometric data is collected. No data is used for parking enforcement activities.

Full lifecycle stewardship: *Data, metadata and information managed by the City of Portland -- and by third parties working on behalf of the City -- that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.*

Personally Identifiable Information is not shared with anyone outside of *Automotus* and is deleted immediately. Aggregated data is shared only with authorized and trained individuals in *Automotus* and only authorized individuals within the City can access these statistics that inherently carry less risk. Client instance, metadata, and debugging data are held by the vendor indefinitely.

Transparency and accountability: *How the City uses, manages and collects information is described clearly, accurately, and shared in an accessible way. Who creates, contributes to, and has access to that information is also clearly documented and communicated to all people who entrust city government with their data and information.*

PBOT's community outreach consists of creating 13 focus groups, partnering with data and technology companies and research institutions, participating in Open Mobility Foundation SMART Grant Collaborative and C40 Cities, briefing the Portland Freight Committee and other interested groups at key project milestones, and briefing Portland's forthcoming Sustainability and Climate Commission at key project milestones. The Focus Groups are: Environmental Justice Focus Group, Privacy and Personal Data Focus Group, Local Business Focus Group, Local Goods Delivery Focus Group, National Freight and Goods Delivery Focus Group, and Internal Subject Matter Expert Working Groups on Sensors and Parking.

Ethical and non-discriminatory use of data: *The City of Portland has an ethical responsibility to provide good and fair stewardship of data and information, following existing non-discriminatory protections, and commits due diligence to understand the impacts of unintended consequences.*

STEWARDSHIP
PBOT is overseeing the project through its lifecycle and is supported by Business Services, IT division, the data management team, and the Policy, Programs and Projects Group.

DUE DLIILGENCE
The City has identified demographics likely impacted by the project. It also plans on communicating via surveys and interviews with community members (e.g., property owners, tenants) and organizational stakeholders (e.g., freight and goods movement stakeholders) to address on-the-ground problems that may emerge. The City will document lessons learned and final outcomes of the pilot project with the community.

Data openness: *Data, metadata and information managed by the City of Portland -- and by third parties working on behalf of the City -- that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.*

The City will make information public on existing operations, fleets, general travel patterns for deliveries & interest, feasibility, willingness to transition fleets to zero-emission alternatives, opportunities, experiences, and impacts of the pilot project. Freight trip generation (number of deliveries received on a given block face/over a given period) will be estimated to understand baseline operations. Based on adopted City policy, there is interest in expanding Zero Emission Vehicles (ZEVs) in local delivery fleets and an awareness of electric and zero-emission delivery modes and options. All data related to this project is de-identified and anonymized. There are no City requirements limiting the sharing of these kinds of data. Data is aggregated enough to prevent significant privacy risk. The Open Curb Data Specification allows for non-employee or non-officials to view aggregated anonymous data from sources associated with the Curb Data Specification as well.

Equitable data management: *The City of Portland will prioritize the needs of marginalized communities regarding data and Information management, which must be considered when designing or implementing programs, services, and policies.*

The community has been considered since the project's conception and will continuously be considered as the project progresses through the 6-month period. Cameras are deployed in a small area downtown with few residential buildings nearby.

Automated Decision Systems *The City will create procedures for reviewing, sharing, assessing, and evaluating City Automated Decision System tools -- including technologies referred to as artificial intelligence -- through the lens of equity, fairness, transparency, and accountability.*

The ML used for this project is for identifying and removing personally identifiable information. This holds a low amount of risk compared to an ML used to decide employment, policing, or judicial decisions.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	Medium

Baseline (B): (T) – Technology level, (U) – use and application level.

Risk type (RT): (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact.

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	I	1.1 Risks due to unauthorized data sharing of PII.	Low	Unlikely	PII is not retained and is deleted immediately right after metadata is taken from it. *Automotus* employees or PBOT employees are unable to see images with personally identifiable information.	Low
T	I	1.2 Risk of not de-identifying information properly or missing PII	Moderate	Unlikely	If there is a failed de-identification, information will be deleted within a certain period. If there is a data breach within that period, identifiable information could be lost; however, this is very unlikely.	Low
T	I	1.3 Transparency Risk from not giving sufficient notice of surveillance.	Low	Unlikely	There is outreach. PBOT may want to give notice to stakeholders and individuals within the capture area of the camera by posting signage. Privacy and Surveillance Focus Group mitigates this risk. Based on the low risk level of data collection, those within the camera's sight are not likely harmed.	Low
U	I	1.4 Risk of using data for other purposes.	Moderate	Possible	The project has a contractual constraint on its data use, including that data will not be shared with law enforcement. Vendor has constrained the data it collects so PBOT does not have access to PII. Information collected in this project will be used only within the constraints of it. This information won't be used for enforcement purposes. Mitigation of this risk must include proper oversight and supervision of information access activity and appropriate training on privacy and information protection of operators.	Medium
U	I	1.5 Risk of personal details being inferred from metadata and risk of re-identification.	Low	Unlikely	This risk is low. Metadata is not labeled in such a way that would create this risk. Metadata is labeled by its general category (e.g., car, EV, pedestrian). Inferences made from metadata depend on how metadata describes the images. In this case, potential inferences would be made from deidentified data (e.g., pedestrian, bicyclist).	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	III	3.1 Chilling Effect.	Low	Possible	A chilling effect is the inhibition or discouragement of the legitimate exercise of natural and legal rights by the threat of legal sanction. With the knowledge of a camera collecting some kind of information or images those on the street may change their behavior. Signs could be used to mitigate this risk.	Low
U	III	3.2 Image and reputation damage due to misuse of the technology	High	Possible	The purpose of these sensors is very specific: verification and monitoring of zero-emissions delivery zones. However, some reputation and public trust damage could happen if there is a privacy breach or a misuse or abuse of this technology. To mitigate this risk, supervisors need to verify proper use of the technology, including any unauthorized access, data sharing, or use different from the original intended use. Reporting and any publicly accessible information dashboards will increase trust, not only from the public, but also from the companies and stakeholders participating in this pilot project. Information in dashboards needs to be updated frequently. Also, the use of onsite and online public signage information about this technology can help nurturing public trust and reduce the number of public records requests. Attaching dashboards that inform what information gets collected and for what purpose can also reduce this risk.	Medium
T	IV	4.1 Cybersecurity breach risk	Medium	Unlikely	Cameras are not connected to digital City infrastructure. Information is retrieved through secure sessions. Vendor quality assurance can be verified by the City's cybersecurity team.	Low
T	IV	4.2 Vandalism, theft, or destruction	Moderate	Unlikely	There is a possibility that someone could tamper with, damage or destroy the camera. However, sensors are mounted on streetlights, high up. it's unlikely this can occur.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	IV	4.3 Risk of reengineering sensor and obtaining information from the device	Moderate	Unlikely	This risk refers to the possibility of reverse engineering a stolen device that could be modified for other purposes. This risk is unlikely, and sensors include their own encryption.	Low
U	V	5.1 Legal risks due to privacy or sensitive information breach	Moderate	Unlikely	There is a possibility of being sued for a public release of information coming from the delivery vehicles that may include the company that owns the vehicle, the type of the vehicle, the time of delivery, the duration of the delivery. The City has added measures to assure that this information is only used for the purposes of this pilot. The project coordinator needs to inform all the companies that will be participating in this pilot about the type of information that is being collected, how this information is protected, and who has access, as well as the actions in cases of a privacy breach. Companies participating in this pilot need to agree to these terms and conditions.	Low
T	VI	6.1 Risks of too expensive commissioning, maintenance, and Decommissioning Costs	Low	Possible	The City could be paying more than necessary due to unintended or unplanned causes. The City can properly plan budgets and services dedicated to service these sensors. Contractual information needs to be included to define who will cover these sensor service costs -- the City, the vendor, or a third party.	Low

Appendix A
Privacy risk assessment framework

Severity (Evaluate for the worst / highest possible impact)				
	A: Low	**B: Moderate**	**C: High**	**D: Extreme**
Individual Privacy Harms	Customer or "telephone book" information collected and could be disclosed (excluding utility customer data, protected by RCW)	Potential disclosure would be limited to non-financial, non-health related information; no personal identifiers (e.g., social security and driver's license #s)	Financial or other highly sensitive information would be collected and disclosable requiring action to remediate negative effects (example: non-HIPAA health data); i.e., credit report management required	Disclosure would result in extreme privacy impacts to highly regulated information; catastrophic public release of financial and personal information requiring credit report monitoring and other remediation
Equity, Disparate Community Impact	Little or no equity impact, technology delivered uniformly without reference to individuals or demographic groups	Accidental or perceived disparate impact to communities by nature of location of technology or service delivered	Intentional disparate equity impact resulting in community concern resulting in privacy harms, media coverage; loss of reputation, legitimacy and trust impacted	Extreme impacts to community, City experiences national media attention; widespread public concern and protest; significant breakdown in business processes associated with damage control
Political, Reputation & Image	Issues could be resolved internally by day-to-day processes; little or no outside stakeholder interest.	Issues could be raised by media and activist community resulting in protests and direct community complaints	Disclosure would likely result in heavy local media coverage; reputation, legitimacy and trust impacted	Likely national and international media coverage; serious public outcry; significant breakdown in business processes associated with mitigation and damage control
City Business, Quality & Infrastructure	Management of disclosure issues would represent negligible business interruption; resolved with no loss of productivity	Issue management would result in brief loss of services; loss of < 1 week service delivery; limited loss of productivity	Significant event; loss of > 1–3-week loss of services; critical service interruption to delivery of infrastructure services	Extreme event; business collapse for department services; loss of > = 3 months of data or productivity; critical business infrastructure loss > 1 month
Legal & Regulatory	Adverse regulatory or legal action not indicated or highly unlikely	Relatively minor incident, regulatory action unlikely; possible legal intervention or consultation for addressing data exposure or loss	Adverse regulatory action likely – i.e., fines and actions associated with CJIS, HIPAA, PCI, NERC, COPPA violations, etc.	Major legislative or regulatory breach; investigation, fines, and prosecution likely; class action or other legal action
Financial Impact	$0-$500 impact; internal costs covered, and no significant external costs incurred	>$500 - $5,000; internal and external costs associated with legal consultation, system rework, overtime	> $5,000 -$50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime	> $50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime

Likelihood analysis.

For assessing probability of risks

Likelihood	Probability
Almost certain	Likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	Likely to occur every 10-20 years
Rare	Has never occurred

Risk Matrix

	Low	Moderate	High	Extreme
Almost Certain				**High**
Likely				
Possible		**Medium**		
Unlikely				
Rare	**Low**			

Appendix B
Definitions

Automated Decision System	A process, set of rules, or tool based on automated processing of data to perform calculations, create new data, or to undertake complex reasoning tasks. This includes advanced methods like artificial intelligence and machine learning, visual perception, speech or facial recognition, and automated translation between languages.
Data	Statistical, factual, quantitative, or qualitative information, in digital or analog form, that is regularly maintained or created by or on behalf of a City bureau and is in a form that can be transmitted or processed.
Data Governance	Definition of policies, processes and framework of accountability to appropriately manage data as a strategic asset.
Digital Age	This current era whereby social, economic and political activities are dependent on information and communication technologies. It is also known as the Information Age or the Digital Era.
Information	Information is the result of Data being processed, organized, structured or presented, allowing it to be used and understood.
Information Protection	A system of Data processing practices related to personally identifiable or identifying Data for the protection of privacy. This includes the management of individual pieces of personal Information, securing Data against unauthorized access, corruption or loss.
Metadata	A set of Data that describes and gives information about other Data, including its description, origination, and accuracy.
Open Data	Data that can be freely accessed, used, reused and redistributed by anyone.
Personal Information	Information about a natural person that is readily identifiable to that specific individual. “personal information,” which include, but are not limited to: • identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers; • payment card industry such as bank account numbers or access codes; • personal health data, such as health history, symptoms of a disease, current health care information, medical device identifiers and serial numbers; • commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; • biometric information; • internet or other electronic network activity information, that includes browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement; • geolocation data, vehicle identifiers (including serial numbers and license plate numbers); • audio, electronic, visual, thermal, olfactory, or similar information; • professional or employment related information; • education information, provided that it is not publicly available; and • inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
HRAR 11.04 Protection of Restricted and Confidential Information	

Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.
Confidential	Information that is made confidential or privileged by law or the disclosure of information that is otherwise prohibited by law or City policy.
Restricted	Some restrictions or limitations on the use of or disclosure of the information.
Principle of proportionality	The principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose
Surveillance Technologies	technologies that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.
Privacy terms	
Effectiveness	This refers to how a specific technology or solution fulfills the pursued objective.
Proportionality	Proportionality is a privacy principle that personal data collected and processed should be adequate, relevant, and limited to that necessary for purpose processed. Proportionality has multiple dimensions. Data collected and used should be adequate, because collecting too little information may lead to incorrect or incomplete information on a data subject. It should also be relevant and limited to what is necessary in relation to the purposes for which it is collected and processed ('data minimization'), both in terms of scope and time (data retention). The proportionality principles consideration of the amount of data to be collected. If excessive data is collected in relation to purposes, then it is disproportionate. Examples: Using biometric data like fingerprints to identify individuals when identity cards would suffice.
data protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy. Data protection should always be applied to all forms of data, whether it be personal or enterprise. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
Frequency of the collection	Periodicity of the data collection.
Privacy safeguards	Measures designed to improve privacy and information protection. It can be represented as below, as, or greater than industry standard and best practices
privacy fundamental rights	Privacy fundamental rights are set to help individuals in being assured of the protection and privacy of their personal data. The General Data Protection Regulation contains a set of 8 privacy fundamental rights. These rights are not legally binding in the US.
Right to information	This right provides the individual with the ability to ask for information about what personal data is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom personal data is shared.

Right to access	This right provides the individual with the ability to get access to personal data that is being processed. This request provides the right for individuals to see or view their own personal data, as well as to request copies of the personal data.
Right to rectification	This right provides the individual with the ability to ask for modifications to personal data in case the individual believes that it is not up to date or accurate.
Right to withdraw consent	This right provides the individual with the ability to withdraw a previously given consent for processing of personal data for a purpose. The request would then require stopping the processing of personal data that was based on the consent provided earlier.
Right to object	This right provides the individual with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that their personal data should not be processed for certain purposes while a legal dispute is ongoing in court.
Right to object to automated processing	This right provides the individual with the ability to object to a decision based on automated processing. Using this right, a customer may ask for this request (for instance, a loan request) to be reviewed manually, because of the believe that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as right to erasure, this right provides the individual with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right and depends on your retention schedule and retention period in line with other applicable laws.
Right for data portability	This right provides the individual with the ability to ask for transfer of his or her personal data. As part of such request, the individual may ask for their personal data to be provided back or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Privacy risk	The term “privacy risk” means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1. Direct or indirect financial loss or economic harm; 2. Physical harm; 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma; 4. Significant inconvenience or expenditure of time; 5. Adverse outcomes or decisions with respect to an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services; 6. Stigmatization or reputational harm; 7. Disruption and intrusion from unwanted commercial communications or contacts; 8. Price discrimination; 9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly: A. Alters that individual’s experiences; B. Limits that individual’s choices; C. Influences that individual’s responses; or D. Predetermines results; or 10. Other adverse consequences that affect an individual’s private life, including private family matters, actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used. 11. Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.
Risk of individual privacy harms	The likelihood that individuals will experience harm or problems resulting from personal data collection and processing
Risk of equity, disparate community impact	The likelihood that specific groups will experience harm or problems resulting from the collection of multiple sources of personal data and their processing.
Risk of political, reputation & image issues	The likelihood that collection or processing of private data may result in harm on professional or personal relationships, harm in reputation or image.
Risk of city business, quality & infrastructure issues	The likelihood that the collection or processing of private data may impact or expose city relationships, agreements, or any other contract, or the quality of those businesses, or built infrastructure
Risk of legal & regulatory issues	The likelihood of any violation of existing laws or regulations by the collection or processing of private information
Risk of financial Impact	The likelihood that ongoing costs in management, collection or processing of private data may become financially inviable or present costs that may not be considered